92 IWAS

Daniel D. Arredondo
92IWAS/CSV
Daniel.arredondo@lackland.af.mil

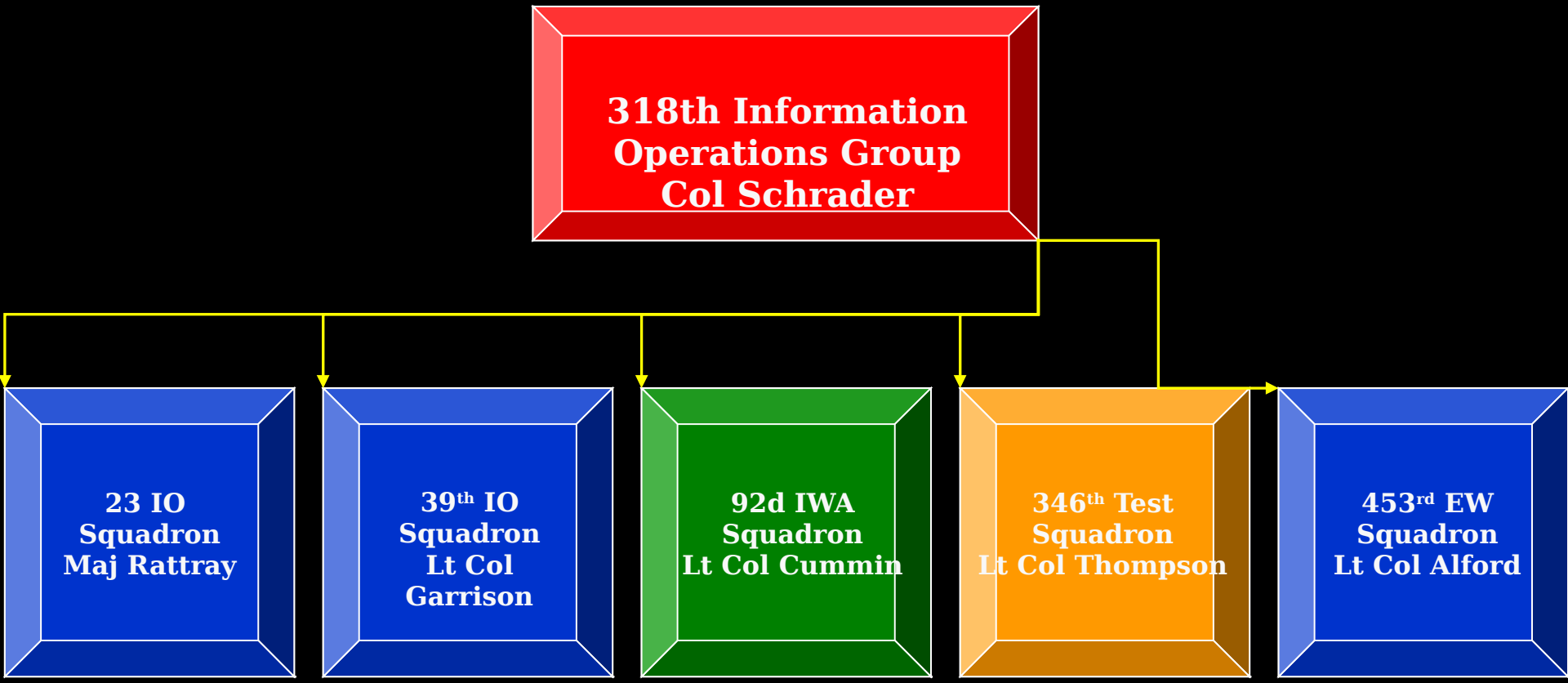
Overview

- Mission
- The Organization
- Assessment Process
- C&A Guidance

92 IWAS Mission Statement

Executes full-spectrum aggressor information warfare operations against aerospace forces through replication of enemy capabilities and tactics. It integrates fully with air and space aggressor forces to represent realistic combat training to the warfighter. 92 IWAS conducts multi-discipline vulnerability assessments in support of MAJCOM operational requirements, and assesses Air Force information networks and systems.

318 IO Group Structure



92 IWAS Structure

92 IWAS

- **Aggressor Operations Flight (AOF)**
- **System Vulnerability Flight (CSV)**
  - **Security Vulnerability Analysis**
  - **System Product Assessment**
  - **New Technologies**
  - **Security Acquisition Program Support**
- **Network Operations Flight (CN0)**
- **Counter Information Programs Flight (CIP)**

92 IWAS Projects

Security Vulnerability Analysis	System Product Assessment	Solution Development	Security Acquisition Program Support
JMPS	Guards & Firewalls	Web Security	F-22 Program
AFMSS	Secure Internet Phone	Database Security	Global Combat Support System (GCSS)
JCALS	Encryptors	Secure Remote E-mail Access	Global Command & Control System (GCCS)
TBMCS	Wireless Technologies	Virtual Private Network (VPN)	

Assessment Process

- The Purpose
- Rules of Engagement
- The Process
- The Product

The Purpose

- To identify and provide guidance to correct and/or mitigate risks for known operating system , application and network vulnerabilities
- Verify Air Force policy compliance
- Review and provide guidance to correct and/or mitigate risks for architectural vulnerabilities

Rules of Engagement

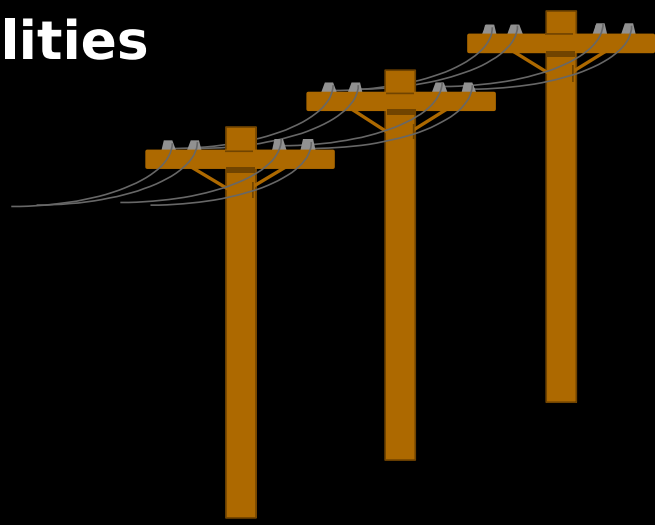
- No configuration changes of any type for the duration of the assessment
- Note changes you would have made and report the incident as if an actual attack were occurring
- AFIWC computers are not to be scanned or attacked
- AFIWC will not conduct denial-of -service attacks

The Process

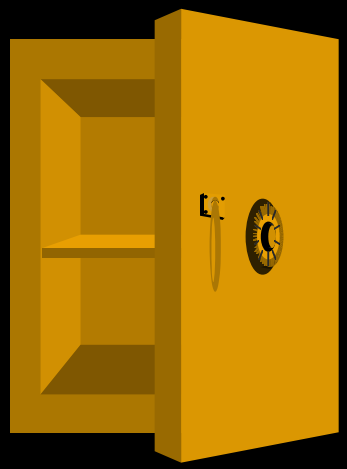
- Phases
  - Remote Assessment
  - Local Assessment

Remote Assessment

- Assess systems from the Internet
  - Emulate remote threat
    - Scan machines to determine operating system and available services
    - Test vulnerable services
    - Routers/firewalls may be blocking some services
    - Test for system level vulnerabilities
    - Dialup modems if applicable



Local Assessment



- Assess systems from local network
  - Emulate insider threat
    - Scan machines to determine operating system and available services
    - Test vulnerable services
    - Test for system level vulnerabilities
  - AFSSI 5027 compliance
  - Review hardware/software configuration of network assets (firewalls, routers, guards, servers, and databases)

The Product

- **Outbrief**
  - **Highlight major findings**
  - **Provide guidance**
- **Formal report**
  - **Detail findings**
  - **Provide guidance and recommendations**
  - **Deliver report to tasker within 90 days**
  - **Report can be used to support C&A process**

C&A Guidance

- National Industrial Security Program (DoD 5220.24)
- Defense Info Tech Security C&A Process (DoD 5200.40)
- AFSSI 5027 – Network Security Policy
- AFM 33-223 – ID & Authentication
- AFI 33-229 – Controlled Access Protection
- AFI 31-401 - INFOSEC Program
- AFI 31-601 - Industrial Security Program
- AFI 31-702 – System Security Program
- AFI 33-114 – Software Management
- AFI 115v1 – Network Management
- AFI 33-119 – Standard Naming Conventions
- AFI 33-129 – Internet Information Transfer
- AFI 33-201 – Communications Security
- AFI 33-332 – Privacy Act Program

C&A Guidance

SYSTEM SECURITY REQUIREMENTS DOCUMENT v1.2

REQ#	DESCRIPTION	REFERENCE OF REQUIREMENT	APPLICABLILITY / COMMENTS	REFERENCE AREA OF ENFORCEMENT / USE	VALIDATION METHOD	COMPLIANCE	ACCEPTABLE
1	Are page maintainer security and access control requests implemented?	AFI 33-129 - Transmission of Information via the Internet, para 4.1.1.14	NO / Web based services are not offered as part of the F-22 weapons system	No Web hosting		N/A	
2	Do web maintainers ensure proper access and security controls are in place and operational?	AFI 33-129 – Transmission of Information via the Internet, para 4.2.1.4	NO / Web based services are not offered as part of the F-22 weapons system	No Web hosting		N/A	
3	Is access to web pages limited by selecting connections for IP addresses ending in .mil or .gov and/or by requiring a password?	AFI 33-129 – Transmission of Information via the Internet, para 8.1.2	NO / Beyond the scope of the F-22 weapons system. This is applicable to base communications	No Router or Proxy ACLs		N/A	
4	Are all internet requests filtered through a proxy server in order to effectively monitor outgoing and incoming activities?	AFI 33-129 – Transmission of Information via the Internet, para 10.2	NO / Beyond the scope of the F-22 weapons system. This is applicable to base communications	No use of web proxy servers		N/A	
5	Are all user Ids and passwords encrypted, such as using Secure Socket Layer (SSL) protocol?	AFI 33-129 – Transmission of Information via the Internet, para 11.1.5	NO / Beyond the scope of the F-22 weapons system. This is applicable to base communications	No F-22 program related user ID/password is passed via the Internet		N/A	
6	Are one-time password systems used for ensuring password integrity?	AFI 33-129 – Transmission of Information via the Internet, para 11.1.5	NO / We are not hosting applications that are available via the Internet	No use of one-time passwords		N/A	
7	Is access to privacy act information protected by the use of password and ID?	AFI 33-129 – Transmission of Information via the Internet, Table 1 AFI 33-332 – Air Force Privacy Act Program, para 7.2	YES	Enforced by the OS of all IMIS workstations and servers Username/password required to access all information	Test: - At the login prompt, type in an invalid username or password - Access to the system should not be given A valid username/password should allow access to the system	YES	
8	If computer-based security is not feasible, have existing safeguards, band controls been enhanced to satisfy security requirements IAW AFMAN 33-229?	AFI 33-202 – Computer Security, para 3.3.1	NO / The computer-based security features available in the IMIS environment meet the Controlled Access Protection (CAP) requirements of AFMAN 33-229	Enforced by the OS Manual auditing of system-generated log files		N/A	
9	Are password-protected screen savers employed when workstations are unattended?	AFI 33-202 – Computer Security, para 3.5.1.3	YES	Enforced by the OS	SCO CMW+ Test: - While at a host, enter <F12> - Select "lock screen" W2K Test:	YES	

CSV

SSAT services and products:

Systems Vulnerability Flight (CSV)

Flight Chief:

POC: Jim Dennis

DSN: 945-5067

Com: (210) 945-5067

e-mail: jim.dennis@lackland.af.mil

Team Composition

Team Members

- Mr. Daniel Arredondo, DSN 945-3393

  daniel.arredondo@lackland.af.mil
- Capt David Olander, DSN 945-3437

  david.olander@lackland.af.mil
- Brett Burley (SAIC), 858-273-2485

  burleyb@saic.com

?Questions?


AIR COMBAT COMMAND
AIR INTELLIGENCE AGENCY
AF INFORMATION WARFARE CENTER
92 IWAS
AGGRESSORS